Bitdefender GravityZone

A unified, multi-layered cybersecurity platform offering advanced endpoint protection, EDR, XDR, and risk management for businesses of all sizes.

https://www.bitdefender.com/

Overview

Bitdefender GravityZone is a comprehensive cybersecurity software suite designed to provide multi-layered protection for endpoints, cloud workloads, and data centers across all major operating systems. It consolidates Endpoint Protection (EPP), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) capabilities into a single, unified platform, managed from a centralized cloud or on-premise console.

Key Benefits and Capabilities:

Advanced Threat Prevention: Utilizes machine learning, behavioral analysis (HyperDetect), and advanced anti-exploit technologies to proactively detect and block new and evolving threats, including zero-day attacks and sophisticated ransomware.
Unified Security Management: Provides a single-pane-of-glass view for deploying, enforcing, and managing security policies across Windows, Mac, Linux, iOS, and Android devices, simplifying security operations for IT teams.
Detection and Response (EDR/XDR): Offers EDR and XDR capabilities with attack forensics and visualization to gain clear understanding of the attack chain, automate incident response, and reduce the mean time to respond (MTTR).
Risk and Compliance Management: Includes a Compliance Manager module with out-of-the-box support for major compliance frameworks like HIPAA, SOC 2, ISO 27001, and GDPR, linking security posture directly to compliance metrics.
Low System Impact: Known for its lightweight agent and low system resource utilization, ensuring protection without compromising device performance.
Target Users and Use Cases: GravityZone is scalable and suitable for businesses ranging from startups and small businesses to mid-market and large enterprises. Its primary use cases include:

Comprehensive Endpoint Protection (EPP).
Advanced Threat Detection and Incident Response (EDR/XDR).
Cloud Workload Security (CWS) for AWS, Azure, GCP.
Data Security and Regulatory Compliance (HIPAA, SOC 2, GDPR).
Securing remote and mobile workforces.

Key Features

- Endpoint Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Full Disk Encryption (FDE)
- Patch Management
- Risk Management and Analytics
- Ransomware Mitigation and Remediation
- Cloud-Based Sandbox Analyzer
- Centralized Cloud/On-Premise Management
- Advanced Anti-Exploit and HyperDetect

Pricing

Model: subscription

Subscription plans start at $77.69 per year for 3 devices (Business Security). Higher tiers like Business Security Premium and Enterprise require custom quotes.

Starting at: USD $77.69

Target Company Size: startup, small, medium, enterprise

Integrations

IBM QRadar (SIEM), Slack, Webhook, Microsoft Azure, VMware NSX-T/V, Amazon EC2, Okta (SSO), Azure AD (SSO)

Compliance & Certifications

HIPAA, SOC 2 Type 2, ISO 27001, GDPR, PCI DSS, CMMC 2.0
